**AY2022/2023 Semester 2- CZ3010 (Solutions)**

1. In the wise man story, at the 20th square, he already had a bag of rice (abt 2^20 grains). How many bags of rice did he earn as his reward?

Ans:

Collect all grains up to 20th square & put it into 1 bag on the 20th square.

Total number of bags (2^20 grains-abt 1 million grains!)

1 + 2^1 + 2^2 + … + 2^44 + 2^45, so roughly 2^46 bags of rice!!! Kingdom bankrupt!

1. (a) Show that the complexity of monoalphabetic substitution (26!) is roughly 2^88. (b)How do you make a monoalphabetic substitution cipher harder to break?

Ans:

First compute log(26!) = log1 + log2 + … + log26 (eg use Excel to add)

Call this number X.

Write 26! = 2^Y.

Hence log(26!) = Y log2 = X

Hence Y = X/log2 = 88.38

1. A 3GHz PC can crack approximately 2^34 work in 1 day. Calculate the time taken (in years) to crack monoalphabetic substitution by brute force using 1 PC. What about cracking time of 1 billion PCs of same specs?

Ans:

Using 1 PC, Cracking time for 2^88 is 2^88/2^34 days = 2^54 days

= 2^54/365 years = 5x 10^13 years!

Using 1 billion PCs, takes, 5x 10^13/10^9 = 50,000 years!

So even NSA and big intel cant crack 88-bit!

1. Why do long keywords, shorter message implies stronger Vigenere cipher?

Ans:

Long keywords lead to lesser observable pattern in ciphertext.

Also more frequency tables needed (length n keyword means n diff freq subst tables)

Shorter msg means stats analysis not accurate

1. General Douglas sends the message ATTACK to his soldiers using a one time pad {GZAMCQ} through email. Suppose attacker sniffed out such a ciphertext. Explain why he/she is not able to decrypt this cipher with 100% certainty, assuming attacker knows it’s from a one-time pad.

Ans:

Adversary will never be sure if plaintext msg is other meaningful 6 letter word such as DEFEND, STATIC etc

1. (a) Why must pad be random?

Ans: real random pad will ensure perfect secrecy, as each bit has equal chance of 0.5 to appear. Totally unpredictable.

(b) Why must pad be not reused again? (asking for a quantitative reasoning)

Ans:

If pad K is reused.

C1 = P1 XOR K

C2 = P2 XOR K (same K)

Then C1 XOR C2 = P1 XOR P2 XOR K XOR K

So C1 XOR C2 = P1 XOR P2, K totally disappear!

1. Johnny English want to make his OTP encryption even harder for attackers. He decides to encrypt twice using 2 different OTPs. Is his method more secure than the usual one?

Ans:

P XOR K1 XOR K2

= P XOR (K1 XOR K2)

(K1 XOR K2) is just another random string of equal length as K1 and K2.

This string is just another same length random string. So no extra security if we encrypt with 2 different one time pad.

1. NSA has intercepted a Vignere ciphertext: {**Y W W L F F D A Q B H L W B G V G R G S N Z D V U}**, and Ethan Hunt has obtained the OTP- **CODE**. **Decrypt this ciphertext.**



1. Use ONLY your mind to create a sequence of 64 random bits, in blocks of 8 bits. Then use any RNG (from OS RNG etc) to generate such a sequence. Then you compare the difference. How many 00000 do you expect to find?

Ans:

P({00000} single run) = (1/2)^5

In a run of 64 entries,

This string can begin on1st, and last possible occurrence is 60th position.

So 60 possibilities.

So expected number of 5 0s = 60\* (1/2)^5 = almost 2.

1. In early IPOD days, some listeners complained hearing the same song within 2 hours although they have 400 songs on their ipod. Assuming 4 min songs on average.

Question: Is the IPOD shuffling random?

**Ans:**

Note that on average, one can hear 30 songs within the 2 hour period under the 4 min average song length rule.

If P(clash) for 30 songs within 400 songs in 2 hour period is > 0.5, clash is expected and claims of non-randomness might not stand.

P(clash) = 1 – P(no clash), which is easier to compute.

Consider general setting N songs in IPOD, k songs within period of consideration.

P( no clash) = N/N\*(N-1)/N\*(N-2)/N\*..\*[N-(k-1)]/N

For our case, N=400, 1 song 4 min implies 30 songs in 2 hours, so k=30.

P(no clash) = 400/400 \* 399/400 \* 371/400 = 0.327 (use EXCEL or programming)

Hence P(clash) = 0.673, a very high chance!

So claims of non-randomness of IPOD shuffle not justified on this ground.

1. Suppose 2 random number generators generate a 8-bit string 11010110 in one portion of the string & another generates 00000000 at another portion. Is the first more random than 00000000?

Ans:

For both events, probability = (1/2)^8 !

So both events are equally likely to happen!

* To most people, the 8-bit string 11010110 is more random than 00000000
* **WRONG!**, although both have the same chance of being generated (namely, (1/2)^8 = 1/256)
* The value 11010110 looks more random than 00000000 because it has the signs typical of a randomly generated value. That is, 11010110 has no obvious pattern.
* But you are actually requiring the bits to follow that specific pattern 11010110 with same probability of occurrence.
* When we see the string 11010110, our brain registers that it has about as many zeros (three) as it does ones (five), just like 55 other 8-bit strings (11111000, 11110100, 11110010, and so on), but only one 8-bit string has eight zeros.
* Because the pattern 3-zeros-and-5-ones is more likely to occur than the pattern 8-zeros, we identify 11010110 as random and 00000000 as non-random, and if a program produces the bits 11010110, you may think that it’s random, even if it’s not.
* Conversely, if a randomized program produces 00000000, you’ll probably doubt that it’s random.